1 Problemset 1 - Supervised Learning

1.1 Linear Classifiers (logistic regression and GDA)

Part a)

Recall that the average empirical loss function of logistic regression is:

$$J(\theta) = -\frac{1}{m}\sum_{i=1}^{m} y^{(i)}\ln(h_\theta(x^{(i)})) + (1-y^{(i)})\ln(1-h_\theta(x^{(i)}))$$

where $y^{(i)} \in \{0,1\}$, $h_\theta(x) = g(\theta^T x)$, and $g(z) = \dfrac{1}{1+e^{-z}}$

Find the Hessian Matrix H of this function, and show that for any vector z, it holds true that:
$$z^T H z \geq 0.$$

Remark:

- The following result means that H is a positive definite matrix. Therefore, J is a convex function and has no local minima other than the global one, hence gradient descent always works well on it.

- Note that log-likelihood function and empirical loss function have different gradients and hessians (only differ the sign).

Solution:
First, observe that:

$$g'(z) = g(z)(1-g(z))$$

By using the derivative of logarithm, we obtain:

$$\frac{\partial}{\partial\theta_j}\ln(h_\theta(x^{(i)})) = x_j^{(i)}(1-h_\theta(x^{(i)}))$$

$$\frac{\partial}{\partial\theta_j}\ln(1-h_\theta(x^{(i)})) = -x_j^{(i)}h_\theta(x^{(i)})$$

Hence for each $j \in \{1,...n\}$:

$$\frac{\partial}{\partial\theta_j}J(\theta) = -\frac{1}{m}\sum_{i=1}^{m} y^{(i)}x_j^{(i)}(1-h_\theta(x^{(i)})) - (1-y^{(i)})x_j^{(i)}h_\theta(x^{(i)})$$

$$= \frac{1}{m}\sum_{i=1}^{m}(h_\theta(x^{(i)})-y^{(i)})x_j^{(i)}$$

Thus the second partial derivatives can be computed as:

$$\frac{\partial^2}{\partial \theta_j \partial \theta_k} J(\theta) = \frac{1}{m} \sum_{i=1}^{m} \frac{\partial}{\partial \theta_k} h_\theta(x^{(i)}) x_j^{(i)} = \frac{1}{m} \sum_{i=1}^{m} h_\theta(x^{(i)})(1 - h_\theta(x^{(i)})) x_j^{(i)} x_k^{(i)}$$

Let D_{pred} be a $m \times m$ matrix where each of its entries is equal to $h_\theta(x^{(i)})(1 - h_\theta(x^{(i)})), i \in \{1, ..., m\}$. By the calculation above, we obtain the Hessian matrix:

$$H = \frac{1}{m} X^T D_{pred} X$$

For the proof that H is positive definite, we can compute $z^T H z$ as:

$$z^T H z = \frac{1}{m} \sum_{i=1}^{m} h_\theta(x^{(i)})(1 - h_\theta(x^{(i)})) \left[(x^{(i)})^T z \right]^2 \geq 0$$

Part b) - Coding Problem

Follow the instructions in src/p01b logreg.py to train a logistic regression classifier using Newton's Method. Starting with $\theta = \vec{0}$, run Newton's Method until the updates to θ are small: Specifically, train until the first iteration k such that $|\theta_k - \theta_{k-1}| < \epsilon$, where $\epsilon = 1 \times 10^{-5}$. Make sure to write your model's predictions to the file specified in the code.

Solution:

```python
class LogisticRegression(LinearModel): #maximize log-likelihood
    def fit(self, x, y):
        m,n = x.shape
        self.theta = np.zeros(n)

        while(True):
            old_theta = self.theta
            h_theta = self.predict(x)

            gradient = np.dot(x.T, y-h_theta)
            hessian = -np.dot(x.T*h_theta*(1-h_theta),x)

            self.theta -= np.dot(np.linalg.inv(hessian),
                gradient)

            if np.linalg.norm(self.theta-old_theta, ord=1) <
                self.eps:
                    break
    def predict(self, x):
        linear_theta = np.dot(x, self.theta)
        return 1/(1+ np.exp(-linear_theta))
```

Result: After training on each dataset then giving the corresponding predictions, we obtain the following statistics:

- Train on "dataset1" and evaluate on "dataset1 valid": **Accuracy** $= 90\%$

- Train on "dataset2" and evaluate on "dataset2 valid": **Accuracy** $= 91\%$
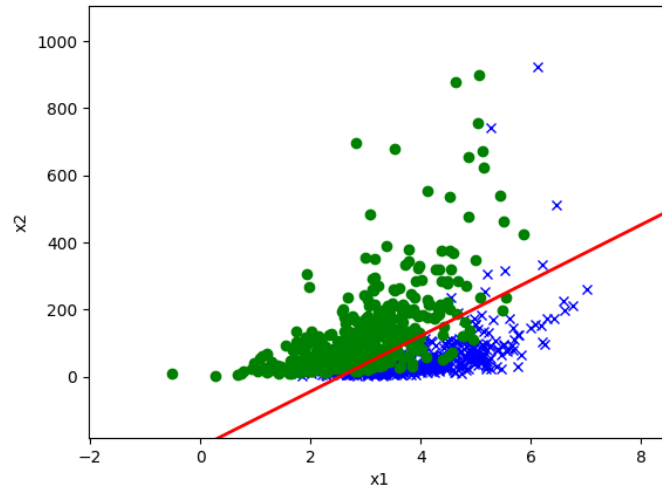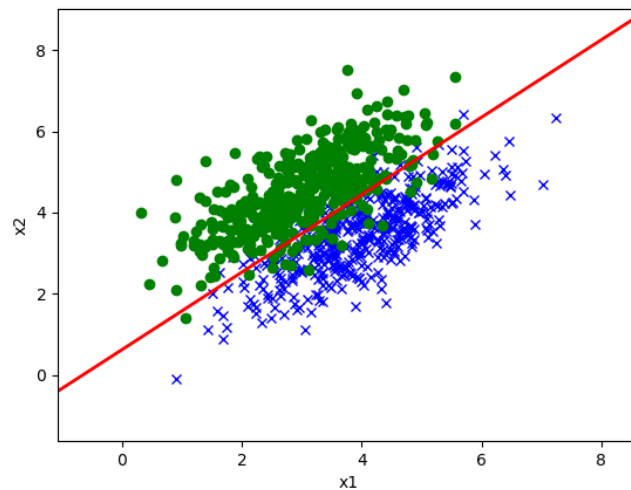
Graph of each dataset:

Figure 1: dataset 1 valid

Figure 2: dataset2 valid

Part c)

Recall that in GDA we model the joint distribution of (x; y) by the following equations:

$$p(y) = \phi^y (1 - \phi)^{1-y}$$

$$p(x \mid y = 0) = \frac{1}{(2\pi)^{n/2}|\Sigma|^{1/2}} \exp(-\frac{1}{2}(x - \mu_0)^T \Sigma^{-1}(x - \mu_0))$$

$$p(x \mid y = 1) = \frac{1}{(2\pi)^{n/2}|\Sigma|^{1/2}} \exp(-\frac{1}{2}(x - \mu_1)^T \Sigma^{-1}(x - \mu_1))$$

where ϕ, μ_0, μ_1 and Σ are the parameters of our model.
Suppose we have already fit ϕ, μ_0, μ_1 and Σ, and now want to predict y given a new point x. To show that GDA results in a classifier that has a linear decision boundary, show the posterior distribution can be written as:

$$p(y = 1 \mid x; parameters) = \frac{1}{1 + \exp(-(\theta^T x + \theta_0))}$$

Where $\theta \in \mathbb{R}^n$ and $\theta_0 \in \mathbb{R}$ are appropriate functions of ϕ, μ_0, μ_1 and Σ.

Solution:

For convenience, we may not include the phrase "parameters" after the conditioned x in our probability density function.
By Bayes's theorem, we have:

$$p(y = 1 \mid x) = \frac{p(x \mid y = 1)p(y = 1)}{p(x)}$$

$$= \frac{p(x \mid y = 1)p(y = 1)}{p(y = 0)p(x \mid y = 0) + p(y = 1)p(x \mid y = 1)}$$

$$= \frac{p(y = 1)}{p(y = 0)\dfrac{p(x \mid y = 0)}{p(x \mid y = 1)} + p(y = 1)}$$

$$= \frac{\phi}{(1 - \phi) \exp\left(\dfrac{1}{2}(x - \mu_1)^T \Sigma^{-1}(x - \mu_1) - \dfrac{1}{2}(x - \mu_0)^T \Sigma^{-1}(x - \mu_0)\right) + \phi}$$

Let $z(\Sigma, \mu_i) = -\frac{1}{2}(x - \mu_i)^T\Sigma^{-1}(x - \mu_i)$. By some computation, we obtain:

$$p(y = 1 \mid x) = \frac{1}{1 + \exp\left[\left(z(\Sigma, \mu_0) - z(\Sigma, \mu_1) - \ln\left(\frac{1 - \phi}{\phi}\right)\right)\right]}$$

$$= \frac{1}{1 + \exp(-(\theta^T x + \theta_0))}$$

Whereas:

$$\theta = -\Sigma^{-1}(\mu_0 - \mu_1)$$

$$\theta_0 = \frac{1}{2}(\mu_0 + \mu_1)^T\Sigma^{-1}(\mu_0 - \mu_1) - ln\left(\frac{1 - \phi}{\phi}\right)$$

Part d)

For this part of the problem only, you may assume n (the dimension of x) is 1, so that $\Sigma = [\sigma^2]$ is just a real number, and likewise the determinant of Σ is given by $|\Sigma| = \sigma^2$. Given the dataset, we claim that the maximum likelihood estimates of the parameters are given by:

$$\phi = \frac{1}{m}\sum_{i=1}^{m} 1\{y^{(i)} = 1\}$$

$$\mu_0 = \frac{\sum_{i=1}^{m} x^{(i)} 1\{y^{(i)} = 0\}}{\sum_{i=1}^{m} 1\{y^{(i)} = 0\}}$$

$$\mu_1 = \frac{\sum_{i=1}^{m} x^{(i)} 1\{y^{(i)} = 1\}}{\sum_{i=1}^{m} 1\{y^{(i)} = 1\}}$$

$$\Sigma = \sum_{i=1}^{m}(x^{(i)} - \mu_{y(i)})(x^{(i)} - \mu_{y(i)})^T$$

The log-likelihood of the data is:

$$\mathcal{L}(\phi, \mu_0, \mu_1, \Sigma) = \sum_{i=1}^{m} \ln p(x^{(i)}, y^{(i)}; \phi, \mu_0, \mu_1, \Sigma) = \sum_{i=1}^{m} ln\left[p(x^{(i)} \mid y^{(i)}; \mu_0, \mu_1, \Sigma)p(y; \phi)\right]$$

By maximizing $\mathcal{L}$ with respect to the four parameters, prove that the maximum likelihood estimates of ϕ, μ_0, μ_1 and Σ are indeed as given in the formulas above. (You may assume that there is at least one positive and one negative example, so that the denominators in the definitions of μ_0 and μ_1 above are non-zero.)

Solution: Again, we will discard the parameters that come after the conditioned variable for convenience. Since $n = 1$, $x^{(i)} \mid y^{(i)}$ obeys the classic Gaussian distribution:

$$p(x^{(i)} \mid y^{(i)}) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left(-\frac{(x^{(i)} - \mu_{y(i)})^2}{2\sigma^2}\right)$$

Also:

$$p(y^{(i)}) = \phi^{1\{y^{(i)}=1\}}(1 - \phi)^{1\{y^{(i)}=0\}}$$

Thus we can rewrite the log-likelihood function as:

$$\sum_{i=1}^{m} -\frac{(x^{(i)} - \mu_{y^{(i)}})^2}{2\sigma^2} - \ln(\sigma\sqrt{2\pi}) + 1\{y^{(i)} = 1\}\ln(\phi) + 1\{y^{(i)} = 0\}\ln(1 - \phi)$$

Computing the partial derivatives:

$$\frac{\partial \phi}{\partial \mathcal{L}} = \sum_{i=1}^{m} \frac{1\{y^{(i)} = 1\}}{\phi} - \frac{1\{y^{(i)} = 0\}}{1 - \phi}$$

$$\frac{\partial \mu_{y^{(i)}}}{\partial \mathcal{L}} = -\frac{1}{\sigma^2} \sum_{i=1}^{m} (\mu_{y^{(i)}} - x^{(i)})$$

$$\frac{\partial \sigma}{\partial \mathcal{L}} = \frac{1}{\sigma^3} \sum_{i=1}^{m} (x^{(i)} - \mu_{y^{(i)}})^2 - \frac{1}{\sigma}$$

Letting the partial derivatives equal to zero, we solve for the parameters to obtain

$$\phi = \frac{1}{m} \sum_{i=1}^{m} 1\{y^{(i)} = 1\}$$

$$\mu_0 = \frac{\sum_{i=1}^{m} x^{(i)} 1\{y^{(i)} = 0\}}{\sum_{i=1}^{m} 1\{y^{(i)} = 0\}}$$

$$\mu_1 = \frac{\sum_{i=1}^{m} x^{(i)} 1\{y^{(i)} = 1\}}{\sum_{i=1}^{m} 1\{y^{(i)} = 1\}}$$

$$\sigma^2 = \sum_{i=1}^{m} (x^{(i)} - \mu_{y^{(i)}})^2$$

Part e) - Coding Problem

In src/p01e gda.py, fill in the code to calculate ϕ, μ_0, μ_1 and Σ, use these parameters to derive θ, and use the resulting GDA model to make predictions on the validation set.

Solution:

```python
import numpy as np
import util

from linear_model import LinearModel
from sklearn.metrics import accuracy_score

class GDA(LinearModel):
    #Gaussian Discriminant Analysis.
    def fit(self, x, y):
        # *** START CODE HERE ***
        m,n = x.shape
        self.theta = np.zeros(n+1)

        # Compute phi, mu_0, mu_1, sigma
        y_1 = sum(y == 1)
        phi = y_1 / m
        mu_0 = np.sum(x[y == 0], axis=0) / (m - y_1)
        mu_1 = np.sum(x[y == 1], axis=0) / y_1
        sigma = ((x[y == 0] - mu_0).T.dot(x[y == 0] - mu_0) + (x[y
            == 1] - mu_1).T.dot(x[y == 1] - mu_1)) / m

        # Compute theta
        sigma_inv = np.linalg.inv(sigma)
        self.theta[0] = 0.5 * (mu_0 + mu_1).dot(sigma_inv).dot(mu_0
            - mu_1) - np.log((1 - phi) / phi)
        self.theta[1:] = sigma_inv.dot(mu_1 - mu_0)

        # Return theta
        return self.theta


    def predict(self, x):
        """Make a prediction given new inputs x.
        Args:
            x: Inputs of shape (m, n).
        Returns:
            Outputs of shape (m,).
        """
        # *** START CODE HERE ***
        linear_theta = x.dot(self.theta) #we added intercept to calc
        return 1/(1 + np.exp(-linear_theta))
```

Result: After training on each dataset then giving the corresponding predictions, we obtain the following statistics:

- Train on "dataset1" and evaluate on "dataset1 valid": **Accuracy** $= 83\%$

- Train on "dataset2" and evaluate on "dataset2 valid": **Accuracy $= 91\%$**

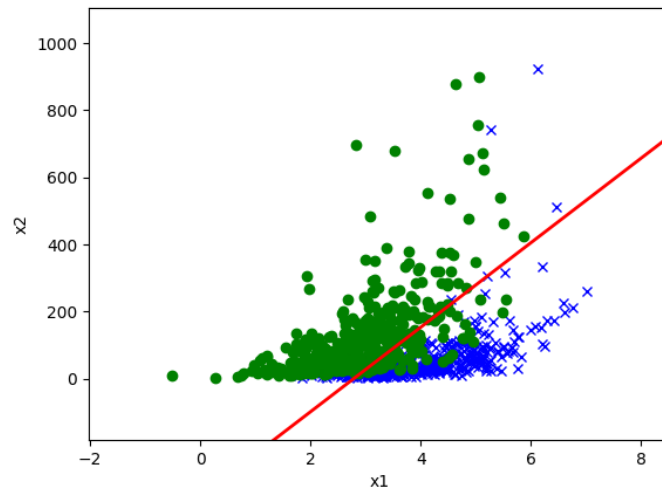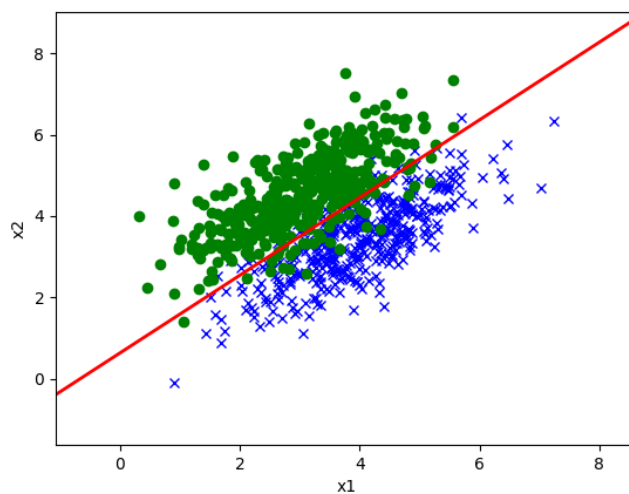**Graph of each dataset:**

Figure 3: dataset 1 valid

Figure 4: dataset2 valid

Part f) + g)

Plot the results of the two algorithms on each dataset. On which dataset does GDA perform worse than Logistic Regression? Why this might be the case?

Solution: Plotting has been shown above. GDA performs worse in the first dataset, with accuracy of 83% comparing to Logistic Regression's 90%. This is probably due to the fact that the input values x do not distribute Gaussianly when conditioned upon y's.

1.2   Incomplete, Positive-Only Labels

In this problem we will consider training binary classifiers in situations where we do not have full access to the labels. In particular, we consider a scenario, which is not too infrequent in real life, where we have labels only for a subset of the positive examples. All the negative examples and the rest of the positive examples are unlabelled. That is, we assume a dataset $\{(x^{(i)}, t^{(i)}, y^{(i)})\}_{i=1}^{m}$, where $t^{(i)} \in \{0,1\}$ is the "true" label, and $y^{(i)} = 1$ if $x^{(i)}$ is labeled, zero otherwise.

All labeled examples are positive, which is to say $p(t^{(i)} = 1 \mid y^{(i)} = 1) = 1$, but unlabeled examples may be positive or negative. Our goal in the problem is to construct a binary classifier h of the true label t, with only access to the partial labels y. In other words, we want to construct h such that $h(x^{(i)}) \approx p(t^{(i)} = 1 \mid x^{(i)})$ as closely as possible, using only x and y.

Real world example: Suppose we maintain a database of proteins which are involved in transmitting signals across membranes. Every example added to the database is involved in a signaling process, but there are many proteins involved in cross-membrane signaling which are missing from the database. It would be useful to train a classifier to identify proteins that should be added to the database. In our notation, each example $x^{(i)}$ corresponds to a protein, $y^{(i)} = 1$ if the protein is in the database and 0 otherwise, and $t^{(i)} = 1$ if the protein is involved in a cross-membrane signaling process and thus should be added to the database, and 0 otherwise.

Part a)

Suppose that each $y^{(i)}$ and $x^{(i)}$ are conditionally independent given $t^{(i)}$:

$$p(y^{(i)} = 1 \mid t^{(i)} = 1, x^{(i)}) = p(y^{(i)} = 1, t^{(i)} = 1)$$

Note this is equivalent to saying that labeled examples were selected uniformly at random from the set of positive examples. Prove that the probability of an example being labeled differs by a constant factor from the probability of an example being positive. That is, show that $p(t^{(i)} = 1 \mid x^{(i)}) = \dfrac{1}{\alpha} p(y^{(i)} = 1 \mid x^{(i)})$, for any value of $x^{(i)}$, where α is a real constant.

Solution: By the rule of conditional probability, we have:

$$p(t^{(i)} = 1 \mid x^{(i)}) = \frac{p(t^{(i)} = 1, x^{(i)})}{p(x^{(i)})}$$

$$p(y^{(i)} = 1 \mid x^{(i)}) = \frac{p(y^{(i)} = 1, x^{(i)})}{p(x^{(i)})}$$

Thus, it suffices to show that the two numerators differ by a real constant.

Again, applying the rule of conditional probability, note that $p(t^{(i)} = 1 \mid y^{(i)} = 1) = 1$:

$$p(y^{(i)} = 1, x^{(i)}) = p(y^{(i)} = 1, x^{(i)}, t^{(i)} = 1) = p(y^{(i)} = 1 \mid t^{(i)} = 1, x^{(i)})p(t^{(i)} = 1, x^{(i)})$$

By using the independence that the problem gave us, we have:

$$p(y^{(i)} = 1, x^{(i)}) = p(y^{(i)} = 1 \mid t^{(i)} = 1)p(t^{(i)} = 1, x^{(i)})$$

Since $p(y^{(i)} = 1 \mid t^{(i)} = 1)$ is independent of $x^{(i)}$, it is a constant. Letting $\alpha = p(y^{(i)} = 1 \mid t^{(i)} = 1)$, we obtain the desired result.

Part b)

Suppose we want to estimate α using a trained classifier h and a held-out validation set V. Let V_+ be the set of labeled (and hence positive) examples in V, given by $V+ = \{x^{(i)} \in V \mid y^{(i)} = 1\}$. Assuming that $h(x^{(i)}) \approx p(y^{(i)} = 1 \mid x^{(i)})$ for all examples $x^{(i)}$, show that:

$$h(x^{(i)}) \approx \alpha, \forall x^{(i)} \in V_+$$

You may assume that $p(t^{(i)} = 1 \mid x^{(i)}) \approx 1$ when $x^{(i)} \in V_+$

Solution: From part a), we have:

$$p(y^{(i)} = 1, x^{(i)}) = p(y^{(i)} = 1 \mid t^{(i)} = 1)p(t^{(i)} = 1, x^{(i)})$$

Thus from $h(x^{(i)}) \approx p(y^{(i)} = 1 \mid x^{(i)})$ and $p(t^{(i)} = 1 \mid x^{(i)}) \approx 1$, we obtain the desired result.

Part c) - Coding Problem

First we will consider the ideal case, where we have access to the true t-labels for training. In **src/p02cde_posonly**, write a logistic regression classifier that uses x_1 and x_2 as input features, and train it using the t-labels (you can ignore the y-labels for this part). Output the trained model's predictions on the test set to the file specified in the code.

Solution:

```
def main(train_path, valid_path, test_path, pred_path):
    #Problem 2: Logistic regression for incomplete, positive-only
        labels.
    pred_path_c = pred_path.replace(WILDCARD, 'c')
    pred_path_d = pred_path.replace(WILDCARD, 'd')
    pred_path_e = pred_path.replace(WILDCARD, 'e')

    # *** START CODE HERE ***


    ###### Prob C
```

```
11
12    x_train, t_train = util.load_dataset(train_path, label_col = 't'
         , add_intercept=True)
13
14    model_t = LogisticRegression(eps = 1e-5)
15    model_t.fit(x_train, t_train)
16
17    x_test, t_test = util.load_dataset(test_path, label_col='t',
         add_intercept=True)
18    util.plot(x_test, t_test, model_t.theta, 'output/p02c.png')
19
20    t_pred = model_t.predictBin(x_test)
21    np.savetxt(pred_path_c, t_pred, fmt='%d')
```

Part d) - Coding Problem

We now consider the case where the t-labels are unavailable, so you only have access to the y-labels at training time. Add to your code in **p02cde_posonly** to re-train the classifier (still using x_1 and x_2 as input features), but using the y-labels only.

Solution:

```
1  def main(train_path, valid_path, test_path, pred_path):
2      pred_path_c = pred_path.replace(WILDCARD, 'c')
3      pred_path_d = pred_path.replace(WILDCARD, 'd')
4      pred_path_e = pred_path.replace(WILDCARD, 'e')
5
6      # *** START CODE HERE ***
7
8      ###### Prob D
9
10     x_train, y_train = util.load_dataset(train_path, label_col='y',
          add_intercept=True)
11
12
13     model_y = LogisticRegression()
14     model_y.fit(x_train, y_train)
15
16     x_test, y_test = util.load_dataset(test_path, label_col='y',
          add_intercept=True)
17     util.plot(x_test, y_test, model_y.theta, 'output/p02d.png')
18
19     y_pred = model_y.predictBin(x_test)
20     np.savetxt(pred_path_d, y_pred, fmt='%d')
```